

<<密码函数的安全性指标分析>>

图书基本信息

书名：<<密码函数的安全性指标分析>>

13位ISBN编号：9787030300089

10位ISBN编号：7030300084

出版时间：2011-2

出版时间：科学出版社

作者：李超 等著

页数：275

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<密码函数的安全性指标分析>>

内容概要

差分均匀度、非线性度、相关免疫阶和代数免疫度分别是刻画密码函数抵抗差分密码攻击、线性密码攻击、相关攻击和代数攻击能力的安全性指标。

《密码函数的安全性指标分析》较为系统地论述了单项安全性指标最优或次优的密码函数的设计与分析，包括完全非线性函数、几乎完全非线性函数、Bent函数、几乎Bent函数和代数免疫度最优的函数的构造、计数和等价性，同时也介绍了非线性度高的弹性函数和代数免疫度最优的函数的构造方法。

本书可以作为密码学专业和信息安全专业高年级本科生和研究生?选修课教材，也可以作为从事密码理论与方法研究的科技人员的参考书。

<<密码函数的安全性指标分析>>

书籍目录

序

前言

第1章 布尔函数与向量值函数

- 1.1 布尔函数及其表示
- 1.2 布尔函数的Walsh变换
- 1.3 布尔函数的安全性指标
- 1.4 向量值函数及其表示
- 1.5 向量值函数的安全性指标
- 1.6 向量值函数和布尔函数的迹表示
- 1.7 Reed-Muller码

参考文献

第2章 完全非线性函数

- 2.1 完全非线性函数的定义
- 2.2 完全非线性函数的原像分布
- 2.3 完全非线性函数的构造
- 2.4 完全非线性函数的等价性
- 2.5 完全非线性函数的应用
 - 2.5.1 基于PN函数的线性码的权分布
 - 2.5.2 基于PN函数的线性码的覆盖结构
 - 2.5.3 基于PN函数的常复合码的构造

参考文献

第3章 几乎完全非线性函数

- 3.1 几乎完全非线性函数的定义与性质
- 3.2 特征为偶数的有限域上的APN函数
 - 3.2.1 APN幂函数
 - 3.2.2 APN多项式函数
- 3.3 特征为奇数的有限域上的APN函数
- 3.4 几乎完全非线性函数的等价性

参考文献

第4章 Bent函数

- 4.1 Bent函数的定义
- 4.2 Bent函数的密码学性质
- 4.3 Bent函数的直接构造法
- 4.4 Bent函数的间接构造法
- 4.5 Bent函数的等价类与计数

参考文献

第5章 几乎Bent函数

- 5.1 几乎Bent函数的定义
- 5.2 几乎Bent函数的Walsh谱和代数次数
- 5.3 几乎Bent函数的等价刻画
- 5.4 几乎Bent函数的构造
 - 5.4.1 幂函数型的几乎Bent函数
 - 5.4.2 多项式型的几乎Bent函数

参考文献

第6章 弹性函数

<<密码函数的安全性指标分析>>

6.1 弹性函数的定义与性质

6.2 弹性函数的构造

6.2.1 直接构造法

6.2.2 递归构造法

6.3 弹性函数的计数

6.3.1 弹性函数的计数上限

6.3.2 弹性函数的计数下限

6.4 向量弹性函数的定义与性质

6.5 向量弹性函数的构造

6.5.1 向量弹性函数的递归构造

6.5.2 高非线性度向量弹性函数的构造

6.5.3 次数大于输出维数的向量弹性函数构造

6.5.4 无线性结构的向量弹性函数的构造

参考文献

第7章 代数免疫度最优的函数

7.1 代数免疫度的定义与性质

7.2 代数免疫度最优的布尔函数的构造

7.2.1 基于支撑包含关系构造MAI函数

7.2.2 基于平面理论构造MAI函数

7.2.3 基于交换基技术构造MAI函数

7.2.4 基于有限域表示构造MAI函数

7.2.5 其他构造

7.3 具有最优代数免疫度的对称布尔函数

7.3.1 具有最优代数免疫度的奇数元对称布尔函数

7.3.2 构造具有最优代数免疫度的偶数元对称布尔函数

7.3.3 具有最优代数免疫度的 2^m 元对称布尔函数

7.3.4 “重量支撑”技术和偶数元对称MAI函数

7.4 向量值函数的代数免疫度

7.4.1 向量值函数三种代数免疫度的定义及其联系

7.4.2 一类具有最优代数免疫度的向量值函数

参考文献

<<密码函数的安全性指标分析>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>